REMARKS

Applicant thanks the Examiner for finding Applicant's arguments presented in the January 19, 2010 Pre-Appeal Brief Request persuasive, and respectfully requests reconsideration of the present application in view of the reasons that follow.

I. Claim Rejections – 35 U.S.C. § 103

A. In the outstanding Office Action, claims 1, 5-7, 9, 10, and 12 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over U.S. Patent Publication No. 2004/0203783 (Wu et al.) in view of U.S. Patent Publication No. 2002/0174335 (Zhang et al.) Applicant traverses the rejection for the reasons set forth below.

Representative independent claim 1 of the present application discloses the following:

> 1. A method, comprising:
> providing access to accessing a public wireless local area network for a user terminal;
> initiating an authentication, authorization and accounting procedure for the user terminal;
> providing an internet access gateway functionality; and
> enforcing an application to switch any traffic provided over internet access to the user terminal in the public wireless local area network to an encrypting security service port, wherein the initiating and enforcing are performed by an access control point.

With regard to independent claims 1, 7, and 10, the Examiner asserted that Wu et al. teaches each and every limitation recited in these claims except for the limitation requiring that the "initiating and enforcing are performed by an access control point." That is, despite Applicant's arguments presented in Applicant's July 10, 2009 Reply and in the Pre-Appeal Brief Request of January 19, 2010 (and the re-opening of prosecution resulting from the Pre-Appeal Brief Request), the Examiner continues to maintain that Wu et al. suggests "enforcing an application to switch any traffic provided over internet access to the user terminal… to an encrypting security service port." Thus it appears that the new grounds of rejection set forth by the Examiner merely attempt to address the limitation requiring that an access control point performs the claimed initiating and enforcement processes.

With regard to Wu et al., the Examiner continued to assert that Figure 2 and paragraphs [0012], [0030], [0031], and [0039]-[0040] of Wu et al. suggest "enforcing an application to switch any traffic provided over internet access to the user terminal… to an encrypting security service port." Applicant again disagrees with the Examiner's position and incorporates herein by reference in their entirety, the arguments presented in Applicant's July 10, 2009 Reply and January 19, 2010 Pre-Appeal Brief Request. That is and again, Wu et al. is directed to a system and method for enabling a wireless terminal to handoff between a first and second access point (AP), where various authentication procedures are performed including certain encryption processes. (*See, e.g.,* Abstract and paragraph [0006] of Wu et al.) However, Applicant yet again submits that the teachings of Wu et al. end at the authentication process. That is, Wu et al. fails to teach or suggest performing any operations after the terminal is authenticated/authorized at the second AP.

Figure 2 and paragraph [0003] of Wu et al. merely teaches that terminals may communicate with a larger network (presumably the Internet) via a WLAN, where an "access point" (AP) is a terminal that "acts as a gateway between the WLAN and the larger network." Applicant submits that this is no more than a general description of WLANs and is neither suggestive nor evidence that the encryption of handoff/session WEP keys between a terminal and an AP is inherently applied to/encompassing of communications over Internet access. Moreover, paragraphs [0004]-[0005] of Wu et al. go further to describe that the reason for the invention described therein is to provide a system and method of authenticating a terminal with an AP in the context of handover from a first AP to a second AP.

Paragraph [0012] of Wu et al. explicitly describes an AP to have a memory that includes instructions to "receive" a packet and "delete" the packet if not encrypted (already) with a handoff WEP key, as well as decrypting and transmitting the packet that is (already) encrypted. Paragraph [0037] of Wu et al. further describes that APs "may only allow the terminal to communication terminal authentication packets with an authentication server. After the terminal has been authenticated… the access points may allow the terminal to communicate date packets via the network." (emphasis added). Moreover, Wu et al. is again clear in that only after a terminal is authenticated (via, e.g., the handover/session WEP key) may it communicate with the network (which as described in paragraph [0003] and interpreted by the Examiner to be, e.g., the Internet), where Wu et al. makes no suggestion that such communication (application) is necessarily enforced to switch such communication traffic over internet access to an encrypting security service port.

In contrast to Wu et al., independent claims 1, 7, and 10 of the present application at least require that an application is enforced to switch any traffic provided over internet access to the UT (in the public WLAN) to an encrypting security service port. That is, after an ACP initiates the AAA procedure for a UT and after the UT is authenticated at the AAA back-end system, the ACP forces applications to switch traffic to an encrypting security service port when the UT tries to access the Internet IP (i.e., any traffic provided over internet access). Again and to be clear, various embodiments of the present application are directed to encrypting those communications/traffic (resulting from applications) between a UT and, e.g., the Internet, that occur after the UT has already been authenticated/authorized with the AP. Hence and again, Wu et al. merely describes an exemplary prior art system/method that merely addresses the initial authentication/authorization of a UT with an AP, not anything that occurs thereafter.

Further still, Applicant respectfully directs the Examiner to MPEP § 707.07(f) which states that "[w]here the applicant traverses any rejection, the examiner should, if he or she repeats the rejection, take note of the applicant 's argument and answer the substance of it." (emphasis added). In this instance, the Examiner has maintained his reasons of rejection at least with regard to the limitation recited in independent claims 1, 7, and 10 of the present application requiring "enforcing an application to switch any traffic provided over internet access to the user terminal... to an encrypting security service port." Thus, Applicant submits that although the Examiner repeated his reasons for rejecting this feature, the Examiner has failed to substantially answer and/or rebut Applicant's arguments presented in at least the Pre-Appeal Brief of January 19, 2010 directed to this feature. Therefore, Applicant respectfully submits that the outstanding Office Action is improper in that it is unresponsive to Applicant's January 19, 2010 arguments and in violation of Section 707(f) of the MPEP.

The Examiner correctly recognized that Wu et al. fails to teach or suggest performing the initiating (of an AAA procedure for the UT) and the enforcing (of an application to switch traffic over internet access to the UT in the PWLAN to an encrypting security service port) at an access control point. However, the Examiner asserted that Zhang et al. cures this deficiency of Wu et al. Applicant respectfully disagrees with the Examiner's position.

Zhang et al. is directed to a system and method of utilizing a user's ISP as a single point of contact for all AAA transactions. (*See, e.g.,* Abstract of Zhang et al.) However, and like Wu et al., Zhang et al. is merely directed to authenticating/authorizing a user/mobile terminal (MT) with an AP, nothing more. That is, and although Zhang et al. generally mentions IPSEC as being used, it is explicitly indicated that IPSEC is merely utilized between the AP and the MT. (*See, e.g.,* paragraphs [0029] and [0068] of Zhang et al.) For example, Zhang et al. provides a "detailed description of an embodiment" beginning at paragraph [0070] of Zhang et al., where it is abundantly clear that the processes described therein are merely directed to authenticating a user/MT to an AP utilizing an ISP. Again, nothing in Zhang et al. teaches or even remotely contemplates actually enforcing, e.g., an application to redirect/switch internet traffic to an encrypting security service port. To wit, paragraph [0086] of Zhang et al., for example, clearly suggests that the preceding description is merely directed to an "authentication session." Paragraphs [0102]-[0104] of Zhang et al. further contradict the Examiner's interpretation thereof, as these sections of Zhang et al. clearly describe how a user/MT is authenticated at a new AP from an old AP during/subsequent to a fast handoff. Again, nothing in these sections of Zhang et al., nor anywhere else in Zhang et al., suggests any type of security/encryption enforcement of traffic over internet access to a UT after the UT has been authenticated/authorized at an AP, regardless of which elements of Zhang et al. might perform the processes described therein.

Because each of claims 5, 6, 9, and 12 of the present application is dependent upon independent claims 1, 7, or 10, Applicant submits that the alleged combination of Wu et al. and Zhang et al. fail to teach each and every limitation recited in claims 5, 6, 9, and 12 for at least the same reasons as discussed above.

In light of the above, Applicant submits that Zhang et al. fails to cure any of the deficiencies of Wu et al., and respectfully requests withdrawal of the rejection of 1, 5-7, 9, 10, and 12 of the present application.

B. In the outstanding Office Action, claims 2, 8, and 11 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Wu et al., Zhang et al., and further in view of U.S. Patent Publication No. 2003/0009691 (Lyons et al.) Applicant traverses the rejection for the reasons set forth below.

With respect to dependent claims 2, 8, and 11, the Examiner correctly recognized that the allegedly combination of Wu et al. and Zhang et al. fails to teach or suggest the use of SSL or TLS security. However, the Examiner asserted that Lyons et al. cures these deficiencies of the alleged combination of Wu et al. and Zhang et al. Applicant respectfully disagrees with the Examiner's assertions.

To the above, Applicant submits that dependent claims 2, 8, and 11 of the present application do not merely require the use of SSL/TLS security. Rather, dependent claims 2, 8, and 11 of the present application require that the "encrypting security service is" SSL/TLS security. Lyons et al. appears to be directed to a centralized clearinghouse for entitlement information in the context of, e.g., Internet purchasing, services provided over the Internet, etc. (*See, e.g.,* Abstract and paragraphs [0001]-[0005] of Lyons et al.) That is, a user or supplier of such Internet purchases/services may access a single "clearinghouse" to verify and/or update that user's/supplier's entitlement to such Internet purchases/services. (*See, e.g.,* paragraph [0007] of Lyons et al.) To effectuate the above, Lyons et al. describes that a clearinghouse may utilize SSL/TLS sessions to authenticate a user with the clearinghouse. However, the clearinghouse of Lyons et al. is <u>not</u> an "encrypting security service." For example, the clearinghouse of Lyons et al. merely "compares the access entry signals to the access information stored on database 100." (*See, e.g.,* paragraph [0016] of Lyons et al.) Thus, Applicant submits that Lyons et al. fails to teach or suggest any sort of "encrypting security service" as required in dependent claims 2, 8, and 11, and certainly not an encrypting security service to be utilized with internet access traffic to a UT in a PWLAN as required in independent claims 1, 7, and 10 of the present application.

Moreover and even if there would be some reason/motivation to combine Lyons et al. with Wu et al. and Zhang et al., Applicant submits that Lyons et al. would still fail to cure any of the aforementioned deficiencies of Wu et al. and/or Zhang et al. That is, because each of claims 2, 8, and 11 of the present application is dependent upon independent claims 1, 7, and 10, respectively, Applicant submits that the alleged combination of Wu et al., Zhang et al, and Lyons et al.. fail to teach each and every limitation recited in claims 2, 8, and 11 for at least the same reasons as discussed above.

In light of the above, Applicant submits that the alleged combination f Wu et al., Zhang et al., and Lyons et al. fails to teach each and every limitation recited in claims 2, 8, and 11 of the present application, and respectfully requests withdrawal of the rejection of these claims.

II. Conclusion

Because none of the references cited by the Examiner, either separately or in combination with each other, teach all of the features recited in independent claims 1, 7, and 10 of the present application, Applicant submits that each of these independent claims is patentable over this prior art. Furthermore, because dependent claims 2, 5, 6, 8, 9, 11, and 12 of the present application are each directly or indirectly dependent upon independent claims 1, 7, or 10, Applicant submits that each of these claims is allowable for at least the same reasons as discussed above, in addition to those discussed regarding dependent claims 2, 8, and 11.

Applicant believes that the present application is now in condition for allowance. Favorable reconsideration of the application as amended is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by the credit card payment instructions in EFS-Web being incorrect or absent, resulting in a rejected or incorrect credit card transaction, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741. If any extensions of time are needed for timely acceptance of papers submitted herewith, Applicant hereby petitions for such extension under 37 C.F.R. §1.136 and authorizes payment of any such extensions fees to Deposit Account No. 19-0741.

Respectfully submitted,

Date July 6, 2010

By /Sanjeev K. Dhand/

G. Peter Albert Jr., Reg. No. 37,268
By Sanjeev K. Dhand, Reg. No. 51,182
Attorney for Applicant

FOLEY & LARDNER LLP
Customer Number: 30542
Telephone: (858) 847-6735
Facsimile: (858) 792-6773